Note

Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search

Michael Adler

> New technologies should lead us to look more closely at just what values the Constitution seeks to preserve.
>
> —Laurence H. Tribe, *The Constitution in Cyberspace*[1]

Black's Law Dictionary defines contraband as "any property which is unlawful to produce or possess."[2] In this Note, I focus on a new class of contraband, digital contraband, in a new enforcement setting, cyberspace. I want to ask what restraints might exist under Fourth Amendment doctrine on the government's ability to discover and prosecute possession of such digital contraband. My attention is focused particularly on an automated, wide-scale search that could hypothetically scan through hundreds of millions of files but would report to authorities only the presence of files containing contraband.

More than just providing insight into law enforcement power in cyberspace, the nature—or lack—of restraints on such a search may provide insights into the Fourth Amendment itself.[3] While the government may never

---

1. Laurence H. Tribe, *The Constitution in Cyberspace: Law And Liberty Beyond the Electronic Frontier*, THE HUMANIST, Sept./Oct. 1991, at 15, 16 (emphasis deleted).

2. BLACK'S LAW DICTIONARY 322 (6th ed. 1990).

3. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

actually conduct the sort of search described in this Note, the Net-wide search provides a concrete and easily visualized case of a "perfect search." This image, in turn, leads us to ask if the power to conduct a "perfect search" would extend unacceptably the reach of government. Justice Potter Stewart once observed that the Fourth Amendment protects "people, not places";[4] the prospect of regular searches for contraband in cyberspace may require us to address the question, "From what?"

Does the Fourth Amendment merely seek to limit the government's ability to discover purely private information, or should the Amendment also serve to restrict the government's access to relevant evidence of criminal activity? In the past, the two limitations were inseparable; the protection from arbitrary searches provided an unacknowledged but potentially quite important pocket of privacy in which individuals might be free to resist the state's demands. The Supreme Court has recognized that the Fourth Amendment constrains the effectiveness of the police, but it has generally cast that constraint as the undesirable but necessary price of protecting innocent citizens from selective application of searches and unjustified invasions of privacy.[5] Even those commentators who have criticized the Court's recent tendency to permit suspicionless searches have framed their arguments in terms of the need to limit police discretion and protect private information the government has no right to learn.[6] As we enter a new age, however, in which it may be possible for the authorities to scan broadly for evidence of illegal conduct without learning anything else, we must ask whether a freedom from such surveillance is not part of the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[7]

This Note begins with a description of a hypothetical Net-wide search, drawing out those features that make it particularly useful for examining Fourth Amendment doctrine. It then analyzes the constitutionality of such a search under the bright-line, property-based standard that dominated Fourth Amendment jurisprudence from the 1880s through the late 1960s,[8] and compares the relatively high level of protection for individuals under that standard to the low level of protection likely to be applied under the current balancing test. Finally, the Note concludes by sketching some of the important

4. Katz v. United States, 389 U.S. 347, 351 (1967).

5. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 137 (1978) ("Each time the exclusionary rule is applied it exacts a substantial social cost for the vindication of Fourth Amendment rights."); *see also* Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development, and Future of the Exclusionary Rule in Search and Seizure Cases*, 83 COLUM. L. REV. 1365, 1393 (1983) ("It is the price the framers anticipated and were willing to pay to ensure the sanctity of the person, the home, and property against unrestrained governmental power.").

6. *See, e.g.*, Thomas A. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 632 (1995) ("Individualized suspicion . . . has served as a bedrock protection against unjustified and arbitrary police actions.").

7. U.S. CONST. amend IV.

8. *See infra* notes 43–59 and accompanying text.

values that inhered in the property-based standard and that would likely militate against any government conduct that approached a "perfect search."

I. THE SEARCH

A. *Life in Cyberspace*

No American with any exposure to the mass media in the 1990s can be unaware of the concept of the "information superhighway."[9] Video, audio, text, and numbers will all be stored and transported as digital data, allowing homes and businesses to connect to each other and to giant information storehouses with an ease never before imaginable. The same computer that balances your checkbook and processes your letters will work as a gateway to a new world; you will be able to call up this week's episode of Star Trek, peruse Shakespearean sonnets or Hegelian philosophy, video conference with your sister in Hawaii, or wander through L.L. Bean's electronic warehouse. And the gateway will work both ways: From your office or the airport, you will be able to connect to your home to get your video messages, update your calendar, grab a video of your dog to show your colleagues, or double-check the address of a friend in Taiwan.

Cyberspace may be described as the nonphysical "place" where electronic communications happen and digital data are located. In its most narrow formulation, "cyberspace" is a synonym for the Internet, "an immense network of networks that connects an estimated twenty million computer users by telephone lines to thousands of electronic information storehouses worldwide."[10] Every "futuristic" possibility described in the preceding paragraph is already a reality on the Internet. Not only can one access great storehouses of information from a machine in one's home or office, but one can access that machine from thousands of miles away.[11]

Of course, if it is possible for one person to access her own machine through public networks, then it is also possible for others to do so. These others may be invited guests allowed into limited areas of the owner's system to share information, or they may be unwanted intruders who have connected to her computer to search for details about her work, her system, and her life.[12] For the inquisitive, a computer's hard drive can be a treasure trove of

---

9. *See* Philip Elmer-DeWitt, *Welcome to Cyberspace: What Is It? Where Is it? And How Do We Get There?*, TIME, Mar. 22, 1995, at 4, 6. ("All of this is being breathlessly reported in the press . . . .").

10. Anne Meredith Fulton, Comment, *Cyberspace and the Internet: Who Will be the Privacy Police?*, 3 COMMLAW CONSPECTUS 63, 63 (1995).

11. Naturally, one's machine can only be accessed when it is on and connected to the network. Increasingly, however, as the computer assimilates the functions of video phone, answering machine, fax machine, mail box, and on-line storehouse, people will be inclined to leave their machines available 24 hours a day.

12. *See* John Markoff, *Taking a Computer Crime to Heart*, N.Y. TIMES, Jan. 28, 1995, § 1, at 33.

information,[13] and if the intruder is sophisticated, the owner may never even realize that anyone unauthorized has accessed her system at all.[14]

As we enter a world in which people increasingly transact and record their lives on computers, and in which those computers increasingly are connected to public networks, the prospect of a search through one's hard drive seems more threatening. Christopher Slobogin and Joseph Schumacher conducted a survey to measure people's subjective sense of the intrusiveness of various governmental actions, and they discovered that the "tapping into [a] corporation's hard drive" seemed almost exactly as intrusive as a "search of [a] college dormitory room."[15] And while today in 1996 one might plausibly claim that anyone on the Internet has voluntarily assumed a lessened expectation of privacy by connecting, this argument becomes increasingly unreasonable the more digital connections become central to our lives.[16] At an almost unbelievable rate, private life is moving into cyberspace: The Internet is growing at a rate of approximately ten percent per month,[17] and people are using the Net not only to exchange ideas and data but to conduct courtships, financial transactions, and more. Corporate offices are going on-line at a similar rate, connecting individual office computers to the vast potential of the Internet. One has only to look at the wave of billion-dollar mergers and deals in the cable, telephone, entertainment, and banking industries to appreciate how many believe that cyberspace will soon be as ubiquitous and indispensable as televisions, telephones, and radios.[18]

---

13. C. Ryan Reetz, Note, *Warrant Requirement for Searches of Computerized Information*, 67 B.U. L. REV. 179, 191-92 (1987).

14. *See, e.g.*, Ellen C. Lesser & Gordon T. Thompson, *How a Hacker Tried to Fool a Security Expert*, N.Y. TIMES, Feb. 22, 1995, at D19 (reporting story of hacker discovered only because of exceptionally sophisticated defense); *see also* Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. REV. 139, 142 (1991).

15. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 763 (1993).

16. Similarly, in 1928 it may have seemed reasonable to assume that anyone with a phone had voluntarily assumed the risk that the line would be tapped. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 466 (1928) ("The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside . . . ."), *overruled by* Katz v. United States, 389 U.S. 347 (1967). Today, no one using the phone believes they are voluntarily accepting such a risk: "To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communications." *Katz*, 389 U.S. at 352.

Put another way, virtually no one would feel that they have assumed the risk that others will examine their voice mail merely because their messages are accessible from remote locations. This is true even though voice mail "hackers" are not uncommon. Neither does one lose an expectation of privacy in one's home because the lock is shoddy and thieves are rampant; if the location invokes Fourth Amendment protection, any barrier to prying eyes suffices. By contrast, if a location does not invoke such protection, no barrier is sufficient. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 178 (1984) (ruling private fields not protected despite fences and "no trespassing" signs).

17. Edward Baig, *Ready to Cruise the Internet?*, BUS. WK., Mar. 28, 1994, at 180, 180.

18. Don L. Boroughs & David Fischer, *Big! Heightened Global Competition, Innovative Technology and Washington's Friendly Regulatory Climate Have Unleashed a New Tidal Wave of Corporate Mergers in America*, U.S. NEWS & WORLD REP., Sept. 11, 1995, at 46, 46–48.

B. *The World of "Digital Contraband"*

Of course, the same digital lines that allow people to send videos of their children to each other also allow them to send videos of child pornography to each other. These same lines that can deliver software instantly from a manufacturer can also be used to exchange, at virtually no cost, perfect copies of pirated music, copyrighted photographs, or unauthorized commercial software. Stolen credit card numbers, telephone access codes, and programs designed specifically to break into other computers[19] inevitably find their way through the network. This is the world of digital contraband.

More precisely, digital contraband is any computer file that, outside of very specific authorized exceptions, cannot be legally possessed. For example, mere ownership of digital videos of child pornography constitutes a federal crime.[20] Similarly, owning a "cracked" copy of a commercial program—one that has been illegally modified to remove licensing protection—is a violation of copyright or contract law.[21] Of course, there are some legal uses of digital contraband,[22] but as with traditional contraband, the mere possession of the analogous digital files would create a strong presumption of illegal activity by the owner.

C. *Law Enforcement Cruises the Net*

Just as possessors of digital contraband may use the Internet to transfer files back to their hard drives, law enforcement agencies might use the fact that such hard drives are connected to the Internet to seek out evidence of illegalities. The interest that a law enforcement officer might have in examining the contents of a hard drive is obvious; the trove of information there may yield important insights into crimes that the owner may have committed.[23] At the same time, the privacy interest that an individual may

---

19. "The ECPA [Electronic Communications Privacy Act] . . . makes it illegal to manufacture, assemble, possess, or sell any device which is primarily useful for the surreptitious interception of electronic communications. . . . Software appears to fall within the conception of a 'device' used to intercept computer communications." Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 93 (1994).

20. 18 U.S.C. § 2252(a)(4)(B) (Supp. 1995) (criminalizing possession of three or more items that contain visual depiction of child pornography if such pornography has been shipped in interstate commerce or produced using materials shipped in interstate commerce—"including by computer"); *see also* Osborne v. Ohio, 495 U.S. 103, 111 (1990) (upholding criminalization of possession of child pornography).

21. It is currently legal to modify programs for archiving purposes. 17 U.S.C. § 117(2) (Supp. 1995). Nevertheless, copy protections exist (and others could be designed) that allow for archiving a program and still restrict the program's use to a particular machine. Any modification to such a protection would violate the law and create a species of digital contraband.

22. For example, a system manager may possess a hacking program to test his own security. *See* 18 U.S.C. § 2512(2)(a) (Supp. 1995). Of course, there are also legitimate research and law enforcement uses for narcotics and automatic weapons.

23. *See, e.g.*, Commonwealth v. Copenhefer, 587 A.2d 1353 (Pa. 1991) (explaining how computer files linked suspect to murder for which he was convicted).

have in the hard drive is also obvious; regardless of whether or not the officer finds evidence of a crime, he may well learn much about the owner's private life in the process of looking through the drive.[24] A number of commentators have written recently about the need for a warrant to ensure limits to the range of the examination—and, consequently, the potential for violation of privacy—possible in a hard drive search.[25]

All of these commentators have assumed that a human investigator will be examining the hard drive to evaluate its contents. Nevertheless, there are certain types of investigations—particularly those focused on digital contraband—in which no human is needed to determine the presence or absence of relevant evidence. A computer program can be designed, for instance, to search through a hard drive and report only the presence or absence of an *exact* copy of a certain piece of illegally modified software.[26] Such an object-targeted search program would ignore any legitimate copy of the commercial software, as well as any copy that was cracked in even a trivially different way.[27] The program would naturally also ignore everything else on the disk, no matter how blatantly illegal—or sensationally intriguing—a human investigator might find that information.

Since such a search program would require an exact copy of the target digital contraband when seeking matching files, the search would be of limited use in targeting particular individuals under suspicion. Say an officer suspects an individual of trafficking in child pornography. The officer could not simply turn the search program loose with the orders that it find any sexually explicit material involving underaged participants.[28] Instead, the officer would need a copy of a particular digital video clip that he believed the suspect possessed, and the search program would tell the officer nothing more than whether that particular clip was on the system. If the suspect had a slightly different video or was clever enough to keep the video encrypted or located on a removable cartridge that was not accessible from the Internet, the search would fail.

However, let us imagine for the moment that the government had acquired technical access sufficient to run such a search program on a large number of

---

24. *See* Randolph Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1222–23 (1995) (discussing possible range of police search).

25. *See, e.g.*, Winick, *supra* note 19; Reetz, *supra* note 13; Sergent, *supra* note 24.

26. Sergent, *supra* note 24, at 1204-05.

27. It would also be possible to design a computer search program that looked for smaller sections within software and therefore reported a much greater amount of information. Such a search would reveal irrelevant information and, consequently, would clearly violate the Fourth Amendment. *See infra* Section II.B. This Note is focused on the more difficult question of a search that can only inform law enforcement of the definitive presence of digital contraband.

28. The officer might turn the program loose with the orders to find the words "child pornography." Nevertheless, not only is the presence of the words "child pornography" insufficient evidence of anything criminal to justify the search, but any search that at heart inquires into the intellectual/verbal/mental beliefs of an individual risks treading on First Amendment values. *Cf.* Stanford v. Texas, 379 U.S. 476, 485–86 (1965) (holding warrant for "books, records, pamphlets" of Texas Communist Party impermissibly broad in light of First Amendment).

networked hard drives simultaneously.[29] Let us further posit that the running of the search program would have a negligible impact on each of the individual systems,[30] and that the search program would report nothing more than the presence or absence of a given piece of digital contraband. Under this scenario, a law enforcement officer who through ordinary means discovered one copy of a piece of digital contraband—a child porn video or a copy of WordPerfect cracked by "Captain Blood"[31]—might infer that since one computer owner has this file, others may as well. The officer might then run a Net-wide search for that contraband. He certainly would not capture every single person who possessed it, but he might nevertheless identify dozens, hundreds, or even thousands of individuals who did have a copy on their computers and for whom he would then have probable cause to request a search warrant.[32]

---

29. There are a number of ways that the government might achieve such technical access. For example, the famous "Internet worm" released by Robert Morris seized control of thousands of systems connected to the Net by exploiting security flaws in Unix systems well known to the National Security Agency and others in the computer security field. *See* KATIE HAFNER & JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER 253-341 (1991). The worm was designed to run unobtrusively in the background, and if it had functioned as Morris originally intended, it might never have been noticed by systems operators.

Still another possibility would be to contract with a private party who had already obtained information about the possession of digital contraband. As part of the test copy for Windows 95, for example, Microsoft included a small program that would by default deliver to Microsoft a record of programs run on the user's machine whenever a user signed onto the new Microsoft Network. *In Short; Thwarting 'Softlifters,'* INFO. WK., May 22, 1995, at 88, 88. Given the Court's conclusion in United States v. Miller, 425 U.S. 435 (1976), that an individual had no Fourth Amendment interest sufficient to object to a seizure of records of his checking account maintained by his bank, it seems likely that the government's purchase or seizure of records from a network or operating-system vendor would be constitutional.

In sum, while such a search is presently hypothetical, it is technically possible—in much the same sense that a free flow of traffic during L.A.'s rush hour is possible. This Note does not argue that such a possibility is likely, but merely that the concrete nature of this hypothetical search allows us to better envision and understand the structure of the Fourth Amendment.

30. One of the first responses that many people seem to have to the prospect of such a search is to fight the hypothetical. They argue that even if this search were possible in theory, there is an unacceptably high probability that the government would botch the search program (as Morris did with his worm) such that the search would damage the target systems. While certainly a *proven* failure would weigh heavily against the use of such a search, the search is at least hypothetically feasible, and one suspects that many would prefer to avoid grappling with the search if any grounds might be found to avoid considering it. The aversion to contemplating this search leads me to believe that many feel a deep uneasiness with the prospect of a successful search of this nature, even if they are unable to articulate a reasoned ground on which to object to such a surgically targeted search.

31. *See Software-Piracy Case in Los Angeles Leads to Felony Charges*, WALL ST. J., Nov. 15, 1995, at B10 (describing capture of software pirate Thomas Nick Alefantes, known as "Captain Blood," and seizure of an estimated $1 million worth of illegally copied software).

32. It might be objected that sophisticated users would either keep their data off-line or encrypt *every* file in order to evade detection. Put another way, this question asks if the mere fact of leaving the data technically accessible amounts to an assumption of risk equivalent to leaving an automatic weapon visible from an outside window. The obvious answer is, that inasmuch as the data is not publicly visible, leaving such data on-line is more analogous to keeping an automatic weapon in an unlocked closet. Given the Court's conclusion in Arizona v. Hicks, 480 U.S. 321 (1987), that merely lifting a turntable to reveal its serial number constituted a search, it seems unlikely that the status of such a search would turn on the extra levels of protection that one might take with data in one's possession. A court should not consider the

The search just described presents a novel set of characteristics:[33] As part of a dragnet search, individuals' hard drives are searched without their permission and without any particularized cause to believe them guilty, and the search scans through a vast amount of very personal information located within people's offices and homes. At the same time, however, the search has a minimal impact on property,[34] produces no false positives, need not be noticeable, and reveals nothing to officials beyond the identity of some individuals who possess this particular piece of digital contraband.[35] How might the Fourth Amendment treat such a search?[36] And what does this tell us about the Fourth Amendment?

II. THE LAW

In the twentieth century, the Supreme Court has set forth two distinct paradigms for interpreting the nature and limits of the Fourth Amendment. Until the late 1960s, the Court grounded its regulation of government searches in the concept of "constitutionally protected areas."[37] Under this view, the Court perceived the Fourth Amendment as a bright-line, property-based standard that required a warrant, supported by probable cause, for most physical trespasses onto private land.[38] However, in the years following its 1961 decision in *Mapp v. Ohio*[39] to vastly widen the scope of the Amendment by applying the exclusionary rule to state police officers, the Court came to recognize that the bright-line standard provided too limited a

absence of encryption on one's personal hard drive to be an assumption of risk any more than the absence of a deadbolt (or even a locked door) is an invitation for an official search of one's home.

33. Although this search is novel in a real life context, Professor Loewy considered the hypothetical of an "evidence-detecting divining rod" that would lead police directly to evidence of wrongdoing. *See* Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1244 (1983). Professor Loewy's conclusion that "there could be no fourth amendment objection to [the rod's] use," *id.* at 1246, is considered in Part III, *infra*.

34. In seizing control of the computer to run the search, the government's program would almost certainly slow other uses of the computer for a brief period, as well as adding a trivial amount of wear to the computer hardware. This impact, while real, is clearly de minimis.

35. In this way, the Net-wide search differs from most searches that enhance natural senses because generally sense-enhanced searches "cannot be as focused as traditional physical searches." David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563, 577 (1990). The search also differs from dog-sniffs, which, while generally accurate and nonintrusive, lack both the broad reach of the Net-wide search and its nonconfrontational character. *See infra* Section II.B.

36. The search, even if legal under the U.S. Constitution's Fourth Amendment, might not be legal under various state versions of the Amendment that have at times been construed more liberally. *See, e.g.*, People v. Dunn, 564 N.E.2d 1054, 1057–58 (N.Y. 1990) (interpreting state constitutional provision worded same as Fourth Amendment as covering broader range of searches). Of course, such state constitutional concerns might not be relevant if the search were conducted by a federal agent.

37. Berger v. New York, 388 U.S. 41, 59 (1967).

38. Under the property standard, the Court recognized only a very limited class of well-defined and long-established exceptions to the warrant requirement, including exigent circumstances, open fields, and (pursuant to the government's obligation to ensure the safety of the roads) automobiles. *See* Vale v. Louisiana, 399 U.S. 30, 34-35 (1970) (listing exceptions).

39. 367 U.S. 643 (1961).

realm of protection from government searches. In three landmark cases, *Katz v. United States*,[40] *Camara v. Municipal Court*,[41] and *Terry v. Ohio*,[42] the Court revised its approach to the Fourth Amendment and attempted to articulate a standard that directly incorporated the values that inhered in a "constitutionally protected area." The resulting balancing method replaced the use of property as a central value, developing instead a values-focused test that weighs the government's interest in a search against the potential for police abuse of discretion and the threat to an individual's privacy inherent in the search.

This part explores the probable status of the Net-wide search first under the bright-line test of the pre-*Katz* Court and then under the current balancing approach. This review of the relevant case law demonstrates that the Net-wide search for digital contraband would be per se unreasonable under the "constitutionally protected areas" standard, and yet per se reasonable under the Court's balancing test as currently formulated. If this analysis is correct, one must ask whether the case of the Net-wide search is nothing more than a very anomalous case in which the pre-*Katz* standard would have provided too much protection, or whether there are in fact potentially important interests implicit in the Fourth Amendment that the Court has thus far failed to include in its balancing test.

A. *The Pre-*Katz *Bright-Line Standard*

In the Supreme Court's first significant examination of the Fourth Amendment, *Boyd v. United States*,[43] the Court found the protection of property to represent the core of the Amendment. In *Boyd*, the firm of E.A. Boyd and Sons was accused of claiming thirty-five more cases of plate glass as exempt from customs duties than it had actually used in constructing federal buildings;[44] the Court faced the question of whether the government could subpoena Boyd's papers for use against the firm. Writing for a majority of seven, Justice Bradley traced the history of the British use of the writs of assistance, by which officers of the Crown were empowered "in their discretion, to search suspected places for smuggled goods."[45] After explaining that the opposition to such sweeping and suspicionless searches was "perhaps the most prominent event which inaugurated the resistance of the colonies,"[46]

40. 389 U.S. 347 (1967).
41. 387 U.S. 523 (1967).
42. 392 U.S. 1 (1968).
43. 116 U.S. 616 (1886). Only two majority opinions prior to *Boyd*, Livingston v. Moore, 32 U.S. 469, 482 (1877), and *Ex Parte* Jackson, 96 U.S. 727, 733 (1877), even mention the Fourth Amendment, and both summarily conclude that the Amendment was violated.
44. *Boyd*, 116 U.S. at 618.
45. *Id.* at 625.
46. *Id.*

Justice Bradley went on to conclude that the protection of an individual's property interest served to restrict "all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life."[47] The Court found that the papers were Boyd's property, and that Boyd alone was entitled to possess them.[48] Even against a "search" as targeted and minimally intrusive as a subpoena, the Court found that one's private property interest outweighed the government's interest in prosecuting crime.[49]

Although later decisions retreated to some extent from *Boyd*'s absolute protection of private property,[50] they retained its property-based orientation. In a series of cases beginning with *Hester v. United States*,[51] the Court mapped out a variety of "constitutionally protected" locations.[52] Under this approach to the Fourth Amendment, government agents might freely inspect any unprotected area, but save for a "few specifically established and well-delineated exceptions,"[53] official intrusion into a protected area required a warrant supported by probable cause.

The property-based model of the Fourth Amendment is well illustrated by *Olmstead v. United States*,[54] a 1928 case that arguably represented the Court's first foray into the jurisprudence of cyberspace.[55] In *Olmstead*, the Court held that federal agents had not violated the Fourth Amendment when they tapped the home and office phones of a suspected bootlegger.[56] A warrant was not necessary for a wire tap, wrote Chief Justice Taft, in large part because "the intervening wires [where the tap was placed] are not part of [the suspect's] house or office."[57] So long as government agents had not pierced the physical borders of the home or office, the Fourth Amendment accorded Olmstead no protection.

Applying the same trespass model over three decades later in *Silverman v. United States*,[58] the Court found that the Fourth Amendment *had* been violated by the insertion of a microphone into an individual's basement heating duct. This small insertion effectively turned the whole heating system into a house-wide microphone. Noting that "the eavesdropping was accomplished by

47. *Id.* at 630.

48. *Id.* at 623.

49. *Id.* at 631–32.

50. *See* Hale v. Henkel, 201 U.S. 43, 70–75 (1906) (listing cases allowing subpoenas of documents and holding documents of any incorporated firm subject to proper subpoena).

51. 265 U.S. 57 (1924) (holding "open fields" not constitutionally protected areas in light of common law "open fields" exception).

52. *See* Lanza v. New York, 370 U.S. 139, 143 (1962) (listing protected areas, including house, office, store, hotel room, automobile, and taxicab, but concluding that visitors' room of jail was not protected area).

53. Katz v. United States, 389 U.S. 347, 357 (1967); *see supra* note 38.

54. 277 U.S. 438 (1928), *overruled by Katz*, 389 U.S. 347 (1967).

55. John Perry Barlow, cofounder of the Electronic Frontier Foundation, once defined cyberspace as "'that place you are in when you are talking on the telephone.'" Elmer-DeWitt, *supra* note 9, at 8.

56. *Olmstead*, 277 U.S. at 466.

57. *Id.* at 465.

58. 365 U.S. 505 (1961).

means of an unauthorized physical penetration into the premises occupied by the petitioners,"[59] the Court found that the penetration converted the eavesdropping into a violation of the Fourth Amendment. This physical intrusion into a protected physical sphere was, for the Court, the decisive difference between *Olmstead* and *Silverman*.

Silverman makes clear that under the property-based standard, a Net-wide search could not withstand Fourth Amendment scrutiny. Any governmental conduct that intruded, even minimally, into a constitutionally protected area without a warrant would violate the Amendment's mandate. The fact that the officer himself is outside the zone would be no more relevant for the Net-wide search than it was for the Court in *Silverman*; the intrusion of the government's search program into the sanctity of a private home or office would trigger the need for probable cause. And the Net-wide search, in invading a subject's hard drive and momentarily seizing control of the computer to execute its scan, would constitute such an intrusion.

The Net-wide search by its very nature precludes a probable cause justification for the intrusion. Because it is simpler and more effective to physically seize a suspect's hard drive than to attempt to access it through the network,[60] an officer who possessed probable cause would secure a traditional warrant for a traditional search. By contrast, law enforcement would use the Net-wide search only when seeking to identify unknown possessors of digital contraband. The search seeks to examine as many drives as it can access, and the likelihood of access bears no relation to the likelihood of illicit files. Under the bright-line test, such a search would be a search without individualized suspicion and—by definition—a violation of the Fourth Amendment.

B. Katz *and Beyond: The Balancing Approach*

In the late 1960s, the Court revised its bright-line approach and developed a balancing test that weighed the government's interest in a search against the costs of the search's invasion of individual privacy. The result, as Louis Seidman has noted, is that "[m]odern Fourth Amendment law focuses on what might be called the 'collateral damage' imposed by searches."[61] Collateral damage includes the involuntary disclosure of personal information not relevant to the investigation, as well as the "violence, disruption, and humiliation"[62] implicit in any search. When the Court speaks of a privacy interest in the context of the Fourth Amendment, it is almost certainly referring to an

---

59. *Id.* at 509.

60. For a discussion of the difficulty of using such a search program to verify the presence of contraband on a particular drive, see *supra* note 28 and accompanying text.

61. Louis Michael Seidman, *The Problem with Privacy's Problem*, 93 MICH. L. REV. 1079, 1086 (1995).

62. *Id.* at 1087.

individual's interest in avoiding either collateral personal revelations or humiliating and potentially violent confrontations with agents of the government. By contrast, where the Court finds none of these collateral damages, it is unlikely to find a violation of privacy.

The Court initiated its revision of the bright-line approach when confronted with a series of cases in which that approach either would have allowed too much collateral damage or, by requiring that the government have probable cause, would have unreasonably hampered important social interests. In *Katz v. United States*,[63] the Court faced the question of whether a wiretap on a public phone was a violation of the Fourth Amendment. Rather than accept the conclusion of *Olmstead* and *Silverman* that the Fourth Amendment's supervision of collateral damage ends at the border of the home or office, the Court instead rejected the absolute line between those areas and the rest of the world. Justice Stewart explained that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[64] Katz's phone conversation could not be intercepted without a warrant.

If *Katz* established that the traditional probable cause standard could apply outside the home and office, *Camara v. Municipal Court*[65] established that searches of the home need not always require probable cause if the intrusion is limited. *Camara* presented the question of whether a housing inspector required a warrant to enter an apartment against the tenant's wishes. Confronted with the municipality's argument that adherence to the traditional probable cause standard would significantly compromise the usefulness of housing inspectors,[66] the Court upheld the search. In light of the unique need for collective inspections and the "relatively limited invasion of privacy"[67] involved in searches targeted at buildings rather than individuals, the Court found that such an "inspection is a 'reasonable' search" of the home despite the lack of individualized suspicion.[68]

The third case, *Terry v. Ohio*,[69] presented the Court with the question of whether a police frisk implicated the Fourth Amendment. Had it chosen to maintain the traditional probable cause requirement, the Court either would have had to allow officers unlimited discretion to frisk (and potentially harass) or it would have had to require probable cause of an officer before he could make sure that a suspect was not armed. Again, the Court chose instead to

63. 389 U.S. 347 (1967).
64. *Id.* at 351–52 (citations omitted).
65. 387 U.S. 523 (1967).
66. *Id.* at 536.
67. *Id.* at 537.
68. *Id.* at 538.
69. 392 U.S. 1 (1968).

modify the traditional test, explaining that "[t]he Fourth Amendment proceeds as much by limitations upon the scope of governmental action as by imposing preconditions upon its initiation."[70] In permitting frisks based on "articulable suspicion,"[71] *Terry* tailored the level of suspicion required to the intrusiveness of the search. This tailoring, in turn, opened the way to a sliding scale in which, the less intrusive the search, the less demanding the procedural requirements for the search to be "reasonable."

Of course, the balancing standard developed in *Katz*, *Camara*, and *Terry* continued to provide the home and office with an exceptionally high level of protection.[72] The similarity of result—and of rhetoric[73]—should not obscure the change in doctrine; the same high level of protection provided by the balancing approach now follows from the fact that any entry into the home or office is virtually certain to impose significant collateral damage. As Professor Seidman notes, when the police conduct such a search, they will almost inevitably interfere with legitimate activity, disrupt personal belongings, and discover personal details that they have no right to learn.[74] Even in a case in which police did no more than place a tracking device inside an object to be brought into a home, which permitted the officers nothing more than the "[i]ndiscriminate monitoring of [the location of] property . . . withdrawn from public view,"[75] the Court has found that the probability of collateral disclosure is significant enough to demand judicial oversight.[76] Private homes are areas that "deserve the most scrupulous protection from government invasion" in order to "protect those intimate activities that the Amendment is intended to shelter from government interference or surveillance."[77]

Nevertheless, although the Court occasionally proclaims that "searches and seizures inside a home without a warrant are presumptively unreasonable,"[78] the presumption that a warrant is required can be rebutted if the Court finds that the social need for a search outweighs the damages it imposes. *Camara*

---

70. *Id.* at 28–29.

71. *Id.* at 31 (Harlan, J., concurring).

72. *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 474–75 (1971); *see also* Payton v. New York, 445 U.S. 573, 603 (1980) (Blackmun, J., concurring) ("Where, however, the warrantless arrest is in the suspect's home, *that same balancing* requires that, absent exigent circumstances, the result be [a Fourth Amendment violation]. The suspect's interest in the sanctity of his home then outweighs the governmental interests." (emphasis added)).

73. *See infra* note 78 and accompanying text.

74. *See* Seidman, *supra* note 61, at 1088-89.

75. United States v. Karo, 468 U.S. 705, 716 (1984).

76. *Id.* That the property in question, a can of ether, was not itself contraband likely played a decisive role in the Court's analysis, since one has no privacy interest in contraband. *See* United States v. Jacobsen, 466 U.S. 109, 123 (1984); *see also infra* text accompanying notes 83–93.

77. Oliver v. United States, 466 U.S. 170, 178–79 (1984).

78. United States v. Karo, 468 U.S. 705, 714–15 (1984); Payton v. New York, 445 U.S. 573, 587 (1980); *see also* Welsh v. Wisconsin, 466 U.S. 740, 749 (1984) ("'[A] search or seizure carried out on a suspect's premises without a warrant is *per se* unreasonable, unless the police can show . . . the presence of "exigent circumstances."'" (quoting Coolidge v. New Hampshire, 403 U.S. 443, 474–75 (1971))).

was one such case. *Griffin v. Wisconsin*,[79] upholding the warrantless search of a probationer's home, was another. In *Griffin*, the Court explained that, although searches of the home are usually "undertaken only pursuant to a warrant . . . we have permitted exceptions when 'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'"[80]

And here the remarkable feature of the Net-wide search for digital contraband becomes apparent: Despite the number of home and office systems searched and despite the total absence of particularized suspicion, the search would result in virtually no collateral damage as currently understood by the Court. There would be no frightening confrontation with authority, no possibility for abuse of discretion, and no disclosure of irrelevant information, private or otherwise, to the police. The Court has noted that "the problem [inherent in the general warrant] is not that of intrusion, per se, but of a general, exploratory rummaging in a person's belongings,"[81] and the remarkable feature of the Net-wide search is that it allows an intrusion without the slightest meaningful rummaging.[82]

As a consequence, under current jurisprudence, such a search would unquestionably be "reasonable." While most balancing tests require the use of judgment and discretion to weigh the different elements, no balancing is required where all the weight is on one side. Even a casual government interest, much less than compelling, might justify this search.

Two decisions in particular, *United States v. Place*[83] and *United States v. Jacobsen*,[84] laid the foundations for this conclusion; together, these cases held that a minimally intrusive practice that reveals "only the presence or absence of . . . contraband"[85] is not recognized as a "search" by the Constitution and hence does not implicate Fourth Amendment scrutiny. The first of these cases, *United States v. Place*, addressed the question of a dog's sniffing of a suspect's luggage for narcotics. The Court noted that since such a sniff "does not require opening the luggage [and] does not expose noncontraband items that would otherwise remain hidden from public

79. 483 U.S. 868 (1987).

80. *Id.* at 873 (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in judgment)). To see the same balance applied to the office, compare Marshall v. Barlow's, Inc., 436 U.S. 307 (1978) (holding warrantless inspections of all businesses impermissible) with New York v. Burger, 482 U.S. 691 (1987) (finding that state interest in preventing car theft justifies warrantless inspection of junkyard office).

81. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971), *quoted in* Andresen v. Maryland, 427 U.S. 463, 480 (1976).

82. Of course, in the most technical of sense, the computer search could be described as both "general" and "exploratory" inasmuch as it scans through *all* files in search of the forbidden one. However, since this scan reveals nothing and thus involves none of the collateral damage generally associated with "rummaging," the Court would almost certainly conclude that it involved no meaningful rummaging.

83. 462 U.S. 696 (1983).

84. 466 U.S. 109 (1984).

85. *Place*, 462 U.S. at 707.

view. . . . the information [so] obtained is limited" to the revelation of contraband.[86] The Court continued:

> In these respects, the canine sniff is *sui generis*. We are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure. Therefore . . . exposure of respondent's luggage . . . to a trained canine did not constitute a [Fourth Amendment] "search". . . .[87]

While some would have read this conclusion as resulting from the dog's use of odors outside the defendant's property,[88] the Court made clear the following year that the decisive fact was "that the governmental conduct [in *Place*] could reveal nothing about noncontraband items."[89] In *Jacobsen*, federal agents tested a small amount of a white powder that Federal Express employees had accidentally discovered in a package. The test destroyed the small sample, but it identified the substance as cocaine. In response to arguments that the test constituted a search, the Court explained that "governmental conduct that can reveal whether a substance is [contraband], and no other arguably 'private' fact, compromises no legitimate privacy interest."[90] As a consequence, the police are free to seek such contraband so long as their search "could, at most, have only a de minimis impact on any protected property interest."[91]

While this conclusion may seem a bright-line rule and a radical departure from the balancing test, it is instead the logical result of that test. A minimally intrusive governmental practice that can reveal only contraband by definition cannot have a recognized collateral effect and so cannot possibly be found unreasonable. While some judges and scholars have objected that being forced to submit to inspection by a large, panting dog inflicts cognizable harm,[92] this criticism is directed at the Court's interpretation of the intrusiveness factor rather than at the test's formulation. If one accepts the Court's implicit

---

86. *Id.*

87. *Id.*

88. *See, e.g.*, United States v. Lewis, 708 F.2d 1078, 1080 (6th Cir. 1983) (holding use of trained dog to detect odors of illegal drugs emanating from luggage and other closed containers not Fourth Amendment violation because odors accessible to public).

89. *Jacobsen*, 466 U.S. at 124 n.24.

90. *Id.* at 123.

91. *Id.* at 125.

92. *See, e.g.*, United States v. DiCesare, 765 F.2d 890, 901–02 (9th Cir. 1985) (Reinhardt, J., concurring); Commonwealth v. Martin, 626 A.2d 556, 563 (Pa. 1993) (Cappy, J., concurring) ("[C]itizens [should be assured] that absent probable cause to believe criminal activity is afoot, they are safe from the probing noses of canine carnivores . . . ."); 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.1(e), at 315 (2d ed. 1987).

assumption that being sniffed by a dog involves neither confrontation nor collateral damage, such a search is per se reasonable.[93]

Unlike the confrontation between dog and target, there is no possible claim of collateral damage in the Net-wide search. As such, the consequence of the Court's reasoning in *Jacobsen* is clear. Since the Net-wide search has only a de minimis impact on the property interests of any individual[94] and reveals nothing "private" beyond the presence of digital contraband, the officers who ran the Net-wide program would not be conducting a Fourth Amendment search. The Court would even be relieved of the need to articulate a "special need" exception from the individualized-suspicion requirement since only "searches" require individualized suspicion.

III. AN UNBALANCED TEST: WHAT'S MISSING?

The conclusion that a Net-wide search would be per se unconstitutional under the earlier standard and yet per se constitutional under the current balancing test highlights a potential and often obscured risk of abandoning a bright-line standard for a balancing approach.[95] While the most recognized drawback of such a shift is the problem of judicial discretion,[96] a less obvious but no less important danger comes to light when the balancing test requires no balancing. This is the possibility that significant interests included *sub rosa*

93. While *Place* and *Jacobsen* did not directly consider dog-sniffs of the home, several lower courts have faced this issue. Although the Second Circuit in United States v. Thomas, 757 F.2d 1359 (2d Cir. 1985), found that *Place* did not apply to sniffs of the home, the Second Circuit seems alone in this position; its *Thomas* opinion has been generally criticized by other courts; *see, e.g.*, United States v. Colyer, 878 F.2d 469, 475 (D.C. Cir. 1989); People v. Dunn, 564 N.E.2d 1054, 1057 (N.Y. 1990) ("[W]e find [the Second Circuit's] attempt to distinguish [*Place*] unpersuasive.").

94. An objection might be raised that, even if the search results in only a de minimis impact on a single individual, the dragnet nature of the search would yield hundreds of thousands of de minimis costs each time the search is run. Commentators have argued in the context of routinized drug tests and sobriety checkpoints that the government's interest in a search's success should only be measured against the sum of costs on society at large. *See, e.g.*, Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis*, 63 N.Y.U. L. REV. 1173, 1196 (1988). At the same time, the Court has regularly concluded that the benefits of such routinized drug tests and sobriety checkpoints are properly weighed against the harm suffered by any single individual. *See* Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (sobriety checkpoint); National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989) (drug tests); Skinner v. Railway Labor Executives Ass'n, 489 U.S. 602 (1989) (same).

95. "[T]he protections intended by the Framers could all too easily disappear in the consideration and balancing of the multifarious circumstances presented by different cases . . . ." Dunaway v. New York, 442 U.S. 200, 213 (1979).

96. Over the last 25 years, commentators and dissenting Justices have repeatedly criticized the Court's application of the *Katz* test. *See* Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1752 n.3 (1994) (listing "impassioned" article titles that reflect "academy's frustration . . . [and] concern"). Any balancing test is vulnerable to both honest differences of opinion among judges and to deliberate result-oriented manipulation; the latter possibility in particular finds Justices and commentators alike claiming that the Court has placed its collective thumb on the side of the government's interests. *See Sitz*, 496 U.S. at 473 (Stevens, J., dissenting); Tracey Maclin, *Constructing Fourth Amendment Principles from the Government Perspective: Whose Amendment Is It, Anyway*, 25 AM. CRIM. L. REV. 669 (1988).

in the original standard will be lost when establishing the factors relevant for balancing.[97] The Court may fail to identify particular elements because those elements are ephemeral, difficult to articulate, or politically unpopular if made explicit.[98] In the context of the Net-wide search, this leads to the question: What, if anything, might be missing in the balancing test as currently articulated? What Fourth Amendment objections might be raised to a computerized search that only uncovered illegalities and neither substantially burdened its targets nor revealed irrelevant personal information?

The natural place to begin this inquiry is with the relation between computers and the home and office, those areas privileged under the traditional bright-line standard. For growing millions of Americans, our computers are the instruments on which we compose and record our thoughts, organize our lives, and maintain our communications with one another. The computer is our diary, our date book, our checkbook, and our letter file. Perforce the very values that one automatically associates with the home and office—the needs for privacy, intimacy, and security—apply to the computers that are located there.

Nevertheless, to say that computers reached through cyberspace deserve the same level of protection as homes and offices only begins to answer the question, for certainly "'[c]rime, even in the privacy of one's own quarters, is, of course, of grave concern to society . . . .'"[99] The Fourth Amendment is not an absolute bar to searches of the home, and as Arnold Loewy notes, it follows from the government's right to search for and seize evidence of crime that "an individual has no inherent right to secrete such evidence."[100] The fact that evidence of a crime is located in the home does not confer upon its possessor the right to withhold that evidence with impunity.

Professor Loewy's conclusion, however, that "if a device could be invented that accurately detected [contraband] and did not disrupt the normal [activities] of people, there could be no fourth amendment objection to its use"[101] only follows if one accepts his axiom that the Fourth Amendment exists solely to insure that the innocent are as free as possible from intrusive searches and seizures. In his view, the innocent should have no objection to being searched by an "evidence-detecting divining rod"[102] so long as the search carries no collateral burdens. While Professor Loewy's axiom seems to be accepted by the current Court,[103] there are at least two independent policy

97. *See* Sundby *supra*, note 96, at 1753–54 ("What if the problem is not with judges improperly doing their Fourth Amendment sums but with the factors themselves?").

98. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 350 (1974) ("[T]he Court cannot always state openly all of the considerations that affect its decisions.").

99. Payton v. New York, 445 U.S. 573, 586 n.24 (1980) (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).

100. Loewy, *supra* note 33, at 1244.

101. *Id.* at 1246.

102. *Id.* at 1244.

103. *See* United States v. Jacobsen, 466 U.S. 109, 123 n.23 (1984) (citing Loewy, *supra* note 33).

interests that might favor the existence of a zone safe from governmental intervention until the government has independently developed evidence of wrongdoing. Inasmuch as these interests are fundamental to the roles of the home and office, they were necessarily incorporated, if tacitly, in the original, bright-line approach. And inasmuch as these interests are fundamental to the well-being of society at large, they ought to be incorporated more fully into the current balancing test.

A. *The Need for Autonomy and Refuge*

Clearly the home and office have always served a principal role as psychological sanctuaries from the outside world. The Net-wide search, like any "evidence-detecting diving rod," raises the question of how much one's sense of sanctuary depends on one's control over the flow of information to the outside world. While at first glance it might appear that the average citizen would not be threatened by any given search for any specific illegality, the fact that we cannot always predict in advance which socially disfavored actions will be criminalized suggests that a Net-wide search lessens one's security in the performance of such actions. Moreover, inasmuch as targets know that the search *could* potentially be directed toward unpopular but noncriminal activities, the search may impose a chilling effect on the exercise of such activities.

The importance of being able to limit the flow of personal information has long been recognized as a key component in the individual's ability to establish a secure relationship with the outside world. In his 1967 book on privacy, Alan Westin argued that privacy should be defined as selective control of access to information about one's self or one's group.[104] This power over information allows the individual some ability to govern how she appears to others, and consequently allows her some control of her interaction with the world.[105] Without that control, the individual's psychological security is endangered, and her assurance of autonomy from the majority is threatened.[106] Recognition of the need for such a space may illuminate the Court's comment in *Boyd* that "[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and

104. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

105. *See* J.M. Balkin, *What Is a Postmodern Constitutionalism?*, 90 MICH. L. REV. 1966, 1988 (1992) ("Our ability alternatively to provide or withhold aspects of our private selves preserves and constitutes our autonomy.").

106. Loss of control over the flow of information about ourselves results in "psychological costs . . . including stress, tension, and anxiety." IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, AND CROWDING 45 (1975).

private property"[107] that violates the Fourth Amendment. To preserve the security of such a realm, the Founders "conferred, as against the Government, the right to be let alone."[108]

Naturally, no person has absolute control over all information about herself, since every time she interacts with another person, she loses control of the information about her that the other person has learned.[109] Furthermore, every time an individual takes an action in public or with public consequences, she runs the risk that others will observe her action or will infer that action from its consequences. Nevertheless, to the extent that an individual's actions in public or with others[110] are voluntary, she knowingly assumes the risk that third parties may learn and divulge such information without her knowledge or consent. This is a natural part of human interaction, and loss of control outside one's home and office is balanced by the existence of a "private enclave where [s]he may lead a private life."[111] The home and office play a critical role in establishing the boundary between the individual's area of security and her area of public life.

It is true that the Net-wide search finds only "relevant" information, but it is society at large and not the individual who defines what is illegal and thus what is relevant. Outside of the limited number of enumerated substantive restrictions, virtually any socially disfavored act can be criminalized at the discretion of the majority; the individual would then retain no control over whether or not information relevant to such an act would be revealed. In this light, one critical problem with the Net-wide search or any other form of an "evidence-detecting divining rod" is that it denies to the individual any space in which she can be sure of controlling information about herself.[112] In short,

---

107. Boyd v. United States, 116 U.S. 616, 630 (1885), *quoted in* Olmstead v. United States, 277 U.S. 438, 474–75 (1928) (Brandeis, J., dissenting).

108. *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting). The realm of privacy not breachable under the bright-line rule also provides a limited solution to the problem of "cumulation." As currently articulated, the Court's balancing test does not account for the fact that little intrusions on any particular individual can accumulate to the point at which the subjective effect of each additional "minimal" intrusion is significantly greater than if it had been the only governmental intrusion. *See* Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 439 (1988). A bright-line test, by minimizing intrusions into the home, provides at least a sanctuary free of accumulating "minimal" intrusions. *See* Wyman v. James, 400 U.S. 309, 335 (1971) (Douglas, J., dissenting) ("The bureaucracy of modern government is not only slow, lumbering, and oppressive; it is omnipresent. It touches everyone's life at numerous points. . . . Isolation is not a constitutional guarantee; but the sanctity of the sanctuary of the *home* is such—as marked and defined by the Fourth Amendment.").

109. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."); *see also* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980) ("Perfect privacy is, of course, impossible in any society.").

110. *See, e.g.*, United States v. White, 401 U.S. 745, 752 (1971) ("[O]ne contemplating illegal activities must realize and risk that his companions may be reporting to the police.").

111. Tehan v. United States *ex rel.* Shott, 382 U.S. 406, 414 n.12 (1966) (quoting United States v. Grunewald, 233 F.2d 556, 581–82 (2d Cir. 1956) (Frank, J., dissenting), *rev'd*, 353 U.S. 391 (1957)).

112. In this respect, the regularized, suspicionless searches by means of metal detectors at airports (or magnetic-strip detectors in libraries) are more acceptable searches, since one acknowledges that one has entered places where others control the environment. *Cf.* Michigan Dep't of State Police v. Sitz, 496 U.S.

no refuge remains in which the individual would not have to worry about the risk of exposure, for as control over the boundary between the area of security and the area of public life disappears, so too does the area of security itself.

In the particular case of the Net-wide search, the need for a zone of control is closely related to a "chilling effect" problem. Almost immediately upon being presented with the hypothetical Net-wide search, many have objected that, if the government can search for copies of child pornography, it can also use the same technique to search for Communist party literature. The obvious response, as the Court observed in *Terry*, is that the Fourth Amendment "cannot properly be invoked to exclude the products of legitimate police investigative techniques on the ground that much conduct which is closely similar involves unwarranted intrusions upon constitutional protections."[113] In other words, the fact that an officer without a warrant may not constitutionally break down one's door does not prohibit an officer with a warrant from so doing.

Nevertheless, if one accepts the definition of a "chilling effect" as a government practice that constricts First Amendment freedoms through "the present or future exercise or threatened exercise of coercive power,"[114] a search that eliminates an individual's control over the boundaries to her most private realms would likely be perceived as a threatening exercise of coercive power. Even if the government were scrupulous in searching only for illegal, rather than merely disfavored, files, targets would nevertheless be aware that at any time and without any warning the government *could* easily and economically widen its scan to include disfavored files.[115] This possibility is compounded by the knowledge that, unlike the general search of colonial times, a widened Net-wide search might take place without the target's knowledge. Inasmuch as an individual's computer is increasingly the tool on which her most private thoughts are formulated, expressed, and recorded, those with dissident thoughts would reasonably feel constricted in articulating them given the awareness that they lack control over even their most personal means of expression.[116]

444, 473 (1990) (Stevens, J., dissenting) (justifying airport and library searches). This is very different from the home or office, where one's security depends on one's control.

113. Terry v. Ohio, 392 U.S. 1, 13 (1968).

114. BLACK'S LAW DICTIONARY 240 (6th ed. 1990).

115. Or that socially disfavored files could suddenly become illegal ones. *See supra* text accompanying note 112.

116. Of course, preventing law enforcement from using such a tool at all will not necessarily prevent rogue departments from creating one. Nevertheless, given the expense of developing, testing, and maintaining such a tool, it seems unlikely that law enforcement would invest in it solely for its illegitimate uses. On the other hand, once such a tool exists, law enforcement need not necessarily misuse the tool for it to intimidate; the mere possibility of misuse may be enough to deter dissident thought. *But cf.* United States v. Karo, 468 U.S. 705, 712 (1984) (noting that police technique "created a *potential* for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment. . . . It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence."). Of course, for this purpose, papers may be

By contrast, a standard that insists that searches of the home and office be based on individualized suspicion would require the government to assemble first a reasonable belief based on information already outside the control of the individual. In other words, not until the individual has acted with the understanding that there could be telltale traces outside of her zone of control, thereby knowingly risking public attention, does she become vulnerable to government intrusion.[117] This bright-line rule, by erecting a substantial barrier at the border to the home, guarantees to each individual the possibility of some control over the flow of personal information because it guarantees her control of a realm in which she need not worry excessively about the presence of others.[118]

B. *A Government of Limited Powers*

A second objection to the Net-wide search might be found in the principle that government should exercise only limited amounts of power. To say that an individual has no right to secrete evidence is not to say that it is desirable or appropriate for the government to have perfect enforcement powers. Justice Jackson, concurring in part in *Watts v. Indiana*, observed that the Constitution and the Bill of Rights were intended to "represent the maximum restrictions upon the power of organized society over the individual that are compatible with the maintenance of organized society itself."[119] This observation suggests that the Fourth Amendment might do more than merely protect the innocent against unwarranted invasion; the Fourth Amendment could be seen as a significant procedural check upon the total power of government.

It is, of course, obvious that the Constitution and Bill of Rights impose specific substantive limits on the power of government—one need look no further than the injunction that "Congress shall make no law respecting an establishment of religion."[120] Equally importantly, however, the Constitution

---

different, since almost by definition they implicate First Amendment values that are to be given broad protection. *But cf.* Stanford v. Texas, 379 U.S. 476, 485 n.16 (1964) (noting that stolen books or ledgers of gambling operation are treated no differently than other evidence).

117. *See* Sundby, *supra* note 96, at 1768 ("When factual probable cause is the core regulating device of government behavior, the Amendment is basically self-regulating because control over the government's ability to intrude rests primarily with the individual. So long as a person does not engage in behavior arising to probable cause . . . individual privacy cannot be invaded."); *see also* Vernonia Sch. Dist. v. Acton, 115 S. Ct. 2386, 2397 (1995) (O'Connor, J., dissenting) ("Searches based on individualized suspicion also afford potential targets considerable control over whether they will, in fact, be searched because a person can avoid such a search by not acting in an objectively suspicious way.").

118. *See* Bowers v. Hardwick, 478 U.S. 186, 206 (1986) (Blackmun, J., dissenting) ("Just as the right to privacy is more than the mere aggregation of a number of entitlements to engage in specific behavior, so too, protecting the physical integrity of the home is more than merely a means of protecting specific activities that often take place there.").

119. 338 U.S. 49, 61 (1949) (Jackson, J., concurring in part and dissenting in part). Clearly, complete obedience to the laws is not required for organized society to function, or society would long since have disappeared.

120. U.S. CONST. amend. I.

provides procedural restrictions on the use of power, such as the bicameralism requirement and the requirement that bills receive either a presidential signature or the approval of two-thirds of the members of both houses of Congress.[121] To allow the government to enact a law without satisfying such procedural safeguards would allow the government to act with unreasonable expediency; the safeguards thus serve to inhibit the growth of power.[122]

In a like manner, the Fourth Amendment can be seen as a deliberate constraint on the power of government. Certainly, as the Court has recognized, "there is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all";[123] what may be new is the realization that the "price" of a minimum of criminality is in fact one of the interests tacitly advanced by the Fourth Amendment. It is worth remembering in this context that the colonists who fought the writs of assistance were arguably at least as angered about *successful* customs searches as they were about unsuccessful customs searches.[124] A government that could reach out and discover wrongdoing whose every trace was hidden in the privacy of the home was a government that had arrogated and concentrated too much power in itself and left its citizens too little freedom.[125]

The protection of property embodied in the *Boyd* decision can be seen as a procedural safeguard that achieved the substantive goal of preserving liberty.[126] More than just demarcating a realm of personal privacy, property provides private parties a source of power independent from—and potentially

---

121. U.S. CONST. art. I, § 7; *see also* INS v. Chadha, 462 U.S. 919, 946–51 (1983) (describing checks and balances).

122. "[T]he guaranties of due process, though . . . considered as procedural safeguards 'against executive usurpation and tyranny,' have in this country 'become bulwarks also against arbitrary legislation.'" Poe v. Ullman, 367 U.S. 497, 541 (1961) (Harlan, J., dissenting) (quoting Hurtado v. California, 110 U.S. 516, 532 (1884)).

123. Arizona v. Hicks, 480 U.S. 321, 329 (1987).

124. *See* Maclin, *supra* note 96, at 705-13 (tracing history of opposition to customs searches and challenging concept that colonists engaged in smuggling were merely "'incidental beneficiaries of a rule not designed for their benefit'" (quoting Loewy, *supra* note 33, at 1248 n.86)).

125. *See* Silas J. Wasserstrom, *The Incredible Shrinking Fourth Amendment*, 21 AM. CRIM. L. REV. 257, 287 (1984) (noting that opposition leading to Bill of Rights came from those who "did not trust their new rulers to exercise unchecked power either benignly or reasonably").

126. In a quite recent article, William Stuntz makes the argument that the Fourth Amendment's principal focus "seems to have been to make it harder to prosecute objectionable crimes—heresy, sedition, or unpopular trade offenses in the seventeenth and eighteenth centuries, regulatory offenses in the late nineteenth century." William Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 394 (1995). In this view, the decision in *Boyd* to prohibit the subpoena of a builder's records played a role in impeding the regulatory state during the *Lochner*-era while having "no effect on the mass of ordinary crimes." *Id.* at 400.

While Professor Stuntz may be correct, *Boyd* was hardly a case whose facts revolved around expanding government regulation. It was rather a case about fraud and customs duties, and however opposed the *Lochner*-era Court may have been to excessive substantive regulation, contractual fraud and customs evasions were hardly the sorts of crimes that the Court was likely to find substantively problematic.

in opposition to—the state.[127] If the Framers' principal concern had been merely specific substantive governmental offenses, they could have drafted an amendment that prohibited only those offenses.[128] Instead, the Framers chose to write an amendment with a reach considerably more broad. Of course, it was a Constitution they were creating, and the knowledge that the Constitution would face developments both novel and unforeseeable no doubt prompted them to select a flexible and comprehensive instrument for limiting government abuses. By choosing an instrument like property that is independent from the government, they ensured a space in which virtually all governmental action might be limited.

Even under a democratic system in which discrete and insular minorities are judicially protected, criminalized actions may nevertheless serve several important functions. For instance, limited violation of a given law may be seen as a form of social insurance, protecting society against the possibility that the government's policy is mistaken. Governmental action might be capricious and ill-considered without violating any substantive right, for as James Wilson explained to the Constitutional Convention, "Laws may be unjust, may be unwise, may be dangerous, may be destructive; and yet not be so unconstitutional as to justify the Judges in refusing to give them effect."[129] To the extent that people defy such a law in spite of the potential penalties, their actions may preserve opportunities that the majority has unthinkingly foreclosed. Furthermore, continual disobedience by a minority may provide society an impetus to reevaluate the law.

Crime in this sense may serve a purpose in the subtle processes of negotiation that takes place between a government and a minority of its citizens, or among citizens themselves where government would prove ineffective. Where minorities have limited influence on decisionmakers, they can often affect policymaking through widespread disobedience of particularly burdensome laws.[130] For example, industrial "slowdowns" may spur labor reform where strikes have been criminalized, draft dodging may undermine support for a controversial war, and squatting may foster land reform when other channels have proven ineffective. On a smaller scale, criminal acts may serve as localized sanctions for damages that the law cannot efficiently police. The farmer in rural Shasta County who castrates a trespassing bull is acting in a criminal manner, but he is also upholding a social norm that encourages

127. *See* Robert C. Ellickson, *Property in Land*, 102 YALE L.J. 1315, 1352 (1993).

128. *See* Payton v. New York, 445 U.S. 573, 583–84 (1980) ("Indeed, as originally proposed . . . the draft contained only one clause which directly imposed limitations on the issuance of warrants . . . .").

129. 2 THE RECORDS OF THE FEDERAL CONVENTION 73 (Max Farrand ed., 2d ed. 1911).

130. *See generally* JAMES SCOTT, WEAPONS OF THE WEAK 35 (1985) (describing wide-scale resistance that becomes "a social movement with no formal organization, no formal leaders, no manifestoes, no dues, no name, and no banner.").

ranchers to control their livestock in order to prevent unnecessary crop damage.[131]

This possibility for reevaluation is particularly significant when social change is at issue. Inasmuch as society criminalizes that which it fears the most, criminal laws occasionally represent a collective prejudice and an irrational desire for the status quo.[132] If we limit all substantive protection of disfavored action to only those actions currently recognized as substantively protected by the Constitution, we limit the possibility of social development. Today we recognize that segregation and McCarthyism were not merely unjust and unwise but actually unconstitutional;[133] had the government been capable of complete enforcement in 1950 of the then-constitutional majority will,[134] quite possibly both would continue today. Instead, "criminal" actions led the way toward social change. As Durkheim once wrote, "[c]rime implies not only that the way remains open to necessary changes but that in certain cases it directly prepares these changes. . . . How many times, indeed, it is only anticipation of future morality—a step toward what will be!"[135]

While clearly much of this change is accomplished through open civil disobedience on explicit moral grounds, much more is accomplished through concealed resistance on often selfish grounds. The actions of the farmer, the draft dodger, the squatter, and the "slow" employee may be justified by an ideology, but the majority of these actions are driven as well by self-interest, and such actions would not be performed if they came at an immediate cost to the actor rather than an immediate gain.[136] Even the civil rights movement in the South depended significantly on the covert support of individuals who stood to benefit from the movement but who could not afford the price of disclosure.[137] Widespread disobedience to the state is difficult enough when there is a risk of serious punishment; it is virtually impossible when the punishment is certain.

In the modern world, the problem of majority dominance is joined by the problem of the increasing size of the regulatory state. Each year, various

131. ROBERT C. ELLICKSON, ORDER WITHOUT LAW 217 (1991).

132. One such example would be anti-miscegenation laws. *See* Loving v. Virginia, 388 U.S. 1 (1967). Another would be anti-homosexuality statutes. *See* RICHARD A. POSNER, SEX AND REASON 346 (1992) ("Statutes which criminalize homosexual behavior express an irrational fear . . . .").

133. *See* Watson v. City of Memphis, 373 U.S. 526, 529 (1963) (asserting "manifest unconstitutionality" of segregation); Baird v. State Bar, 401 U.S. 1, 6 (1971) (plurality opinion) ("The First Amendment's protection of association prohibits a State from excluding a person from a profession or punishing him solely because he is a member of a particular political organization or because he holds certain beliefs.").

134. *See, e.g.*, Adler v. Board of Educ., 342 U.S. 485 (1952) (finding no infirmity in law prohibiting municipal employment for members of Communist party).

135. ÉMILE DURKHEIM, THE RULES OF SOCIOLOGICAL METHOD 71 (George E.G. Catlin ed., Sarah A. Solovay & John H. Mueller trans., 1938) (1895).

136. *See, e.g.*, ELLICKSON, *supra* note 131, at 217 ("An informal enforcer . . . wants to be able to act surreptitiously.").

137. *See, e.g.*, Bates v. City of Little Rock, 361 U.S. 516, 520–22 (1960) (describing danger attendant upon revelation of NAACP membership list).

branches of government enact large quantities of regulations, the vast majority of which the average individual neither considers before they are enacted nor knows about once they are in force. The sum total of such law is staggering: One commentator estimates that there are over 300,000 regulations at the federal level *alone* that are criminally enforceable.[138] Even if every law were clear on its face, and even if there were no objections to the substantive nature of any of the laws, the sheer multitude of laws and regulations would make it difficult for an individual to be aware of, much less in compliance with, every one.[139]

As a consequence, at any given time a very large number of Americans are in violation of some law, and such violations expose them to the punitive power of the state.[140] Were the government suddenly to become aware of these transgressions, the individual's reputation, property, and even personal liberty would be subject to the discretion of the state.[141] That discretion could be turned against the individual and used to discourage disfavored conduct totally unrelated to the original offense. Only the fact that the vast majority of these transgressions will never be discovered allows an individual to feel that she might live without a constant concern for her legal status.[142] Only this limitation on the reach of government permits her to feel secure in her autonomy.

The problem is compounded by the fact that the range of a given law is often unclear. Examples abound of daily affairs in which it is difficult to know when one is in violation of the law: Is a given use of copyrighted material fair use? Does a given meal constitute a tax-deductible expense?[143] Does a suggestive picture of a child constitute child pornography?[144] Does

---

138. *See* Thomas Leary, *The Commission's New Option that Favors Judicial Discretion in Sentencing*, 3 FED. SENTENCING REP. 142, 144 n.10 (1990) (citing comments of Stanley S. Arkin at October 1990 conference at George Mason University).

139. *Cf.* James V. DeLong, *The Criminalization of Just About Everything*, AM. ENTERPRISE, Mar./Apr. 1994, at 26, 29 ("Governmental speakers at legal seminars concede that there are so many environmental requirements and they are so complex that no one can be in compliance.").

140. *See* Stephen J. Adler & Wade Lambert, *Common Criminals: Just About Everyone Violates Some Laws, Even Model Citizens*, WALL ST. J., Mar. 12, 1993, at A1.

141. *See id.* ("The two authors . . . admit, between them, to having committed 16 of the 25 offenses listed on the chart on page A4, carrying maximum jail time of 15 years and fines of as much as $30,000. Most of the dozens of people interviewed . . . have violated eight or more.").

142. *Cf.* DeLong, *supra* note 139, at 30 ("[F]ew people in any position of responsibility are free of an ominous sense of being subject to [legal] risks they cannot assess or prevent, no matter how honestly they try.").

143. Approximately six million Americans, including many in the same households that are connecting to the Internet, now keep their personal accounting on the program Quicken. John McCormick, *Our Man Versus the Quicken Cult*, NEWSWEEK, Feb. 27, 1995, at 49, 49. Under the same logic that applies to the Net-wide search, an automated computer program that checked one's Quicken records against one's tax return would be constitutional so long as the program revealed nothing to government agents beyond noncompliance.

144. *See, e.g.*, Paula Span, *Sexy Calvin Klein Ads Spark FBI Inquiry: Investigation To Determine if Child Exploitation Laws Were Violated*, WASH. POST, Sept. 9, 1995, at A1.

employing a teen part-time require Social Security payments?[145] In America today, how many people could feel certain that they have violated no criminally sanctionable law in the past year?

The protection of a secure zone around the home and office serves to make some disobedience possible by allowing a space in which the government's enforcement power is handicapped. In light of this, it will perhaps be objected that this zone begins to sound like the general right of privacy considered and rejected by the Court in *Bowers v. Hardwick*.[146] While it is certainly true that such an expansive privacy right would achieve the goals posited here, such a strong conclusion is far from necessary. Legislatures might still outlaw activities that take place in the home and office, and law enforcement might still prosecute such offenses. Individuals who act in opposition to the law must do so knowing that society disapproves of their actions and that they run the risk of punishment. Accomplices—or the effects outside the protected areas of actions within—may betray the crime to law enforcement. Individuals discovered through such revelations would be appropriately subject to criminal punishment.

Nevertheless, in the interests of preserving the possibility of a low level of criminal activity and of allowing individuals some freedom from the punitive power of the state, the Fourth Amendment might be seen as militating against any search technique that left society little flexibility. To some it may seem paradoxical for a court to consider the need for disobedience. Of course, to some it has always seemed a contradiction that the Constitution should protect the right of individuals to support manifestly nondemocratic ideals.[147] In both cases, the Constitution permits opposition to the majority on the understanding that a small dose of fundamental opposition keeps a democracy balanced and functioning.

CONCLUSION: A NEW BALANCE

Let us assume that the Court, faced with the case of the Net-wide search, recognized that the old standard had provided protections for important interests, including the individual need for a zone of autonomy and the collective need for a potential for disobedience, that were not incorporated into the present test.[148] While one possibility would be a return to the pre-*Katz*,

145. Payroll accounting packages might also be searched. *See supra* note 143 (discussion of Quicken).

146. 478 U.S. 186, 195 (1986) ("[I]llegal conduct is not always immunized whenever it occurs in the home. Victimless crimes, such as the possession and use of illegal drugs, do not escape the law where they are committed at home.").

147. *Compare* HADLEY ARKES, THE PHILOSOPHER IN THE CITY 81 (1981) (finding contradiction in protection of ideas that deny democratic truths) *with* Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam) (protecting mere advocacy of anti-constitutional goals).

148. Professor Sundby argues that the Fourth Amendment might be seen as mitigating against actions that undercut the mutual trust between the state and the citizen. In his view, "a crucial part of American

bright-line standard, such an approach would generate many more problems than it would solve. The Warren Court abandoned the bright-line approach in the face of the growing complexity of modern life, and that approach would be still less workable today.

In my view, the appropriate solution would be to retain the balancing approach and modify the test to include these interests. Once included in the test, these factors would create a presumption against the Net-wide search that could only be overcome by a strong showing that the digital contraband in question represented an immediate danger to life and limb. Justice Jackson once wrote, "if we are to make judicial exceptions to the Fourth Amendment . . . it seems to me they should depend somewhat on the gravity of the offense."[149] Although the Court has never incorporated Justice Jackson's position into the definition of probable cause as such, the Court has appropriately achieved the same result by including the weight of the government's needs as a factor in determining the level of individualized suspicion required for a given search.

As a consequence, while the Fourth Amendment ought to prevent routine uses of the Net-wide search for nonviolent criminals such as software pirates or possessors of child pornography, it would not have prevented a Net-wide search on the day the Unabomber delivered his manifesto to the *New York Times* and the *Washington Post*.[150] On the extraordinary occasion when a search might yield reliable evidence tying its possessor directly to violent crime, the interests protected by the Fourth Amendment clearly yield. Not only is there a negligible social interest in reevaluating the value of violent disobedience, but even the threat to one's autonomy is less serious in the case of physical violence to others. Such crimes are comparatively rare, and we need have little fear that the majority will suddenly criminalize something previously personal. Although the use of the Net-wide search for violent crime restricts the area of the individual's autonomy slightly, a firm limitation to immediate threats of violence would present little threat of future government expansion.

The prospect of a Net-wide search in cyberspace presents us with a vision of a search that might cheaply, easily, and effectively scan through areas as sensitive and central to our personal security as our diaries, our checkbooks,

---

democracy's staying power is the role of reciprocal government-citizen trust in fostering the confidence among all individuals that they have the opportunities and capabilities to participate meaningfully in society." Sundby, *supra* note 96, at 1779. In a sense, the need for disobedience and the need for trust are flip sides of the same coin; in both cases, the state must consider the individual as, to some degree, a sovereign capable of individual choice rather than an obedient subordinate.

149. Brinegar v. United States, 338 U.S. 160, 183 (1949) (Jackson, J., dissenting in part).

150. Such a search would have been possible, since at the moment the manifesto was delivered, presumably only the *New York Times*, the *Washington Post*, *Penthouse*, and the Unabomber himself possessed it. *See* John Elson, *Murderer's Manifesto: Threatening More Attacks, Unabomber Issues a Screed Against Technology*, TIME, July 10, 1995, at 32, 32.

our calendars, and our correspondence. The prospect of such a surgical search[151] thus requires us to ask, in essence, whether there is not a limit to even the legitimate power that might be exercised by the state, and if so, what the contours of that limit might look like. In this respect, it is important to remember that while "[t]he touchstone of [the Court's] analysis under the Fourth Amendment is always . . . reasonableness,"[152] the Founders' ultimate desire was not that the government be reasonable but rather that the people be *secure* in their persons, houses, papers, and effects.

The vision implicit in the Fourth Amendment reaches beyond the dictates of simply seeking more efficient enforcement techniques. The Court once noted that neither the Fourth nor the Fifth Amendment is "an adjunct to the ascertainment of truth. . . . [Rather, those privileges] stand[] as a protection of quite different constitutional values—values reflecting the concern of our society for the right of each individual to be left alone."[153] The values of one's home and office as a psychological refuge and as a source of power independent of the government represent a pair of interests protected by the property-model of the Fourth Amendment. The continuing importance of these interests suggests that there is indeed an outer bound beyond which a constitutional government cannot reasonably expand, and that as a consequence the list of factors to be balanced is seriously incomplete. Until now, these omissions have been largely obscured by other, serendipitous limitations on governmental conduct, but as technology makes possible more economical and more targeted searches, the Court will need to expand its current test if the balancing approach is to continue to serve the fundamental purposes of the Fourth Amendment.

151. While the Net-wide search is one such surgically targeted search, other technologies might achieve the same effect. One reported case on thermal scanners suggests that the operator of a thermal scanner can "determine the level of coffee in a cup, and tear ducts on a human face" from outside the home. United States v. Field, 855 F. Supp. 1518, 1531 (W.D. Wis. 1994). While a human operator might thus discover private facts, a computer could in theory be attached to the scanner and report only evidence of criminal activity (like the thermal patters of a marijuana plant). The resulting device would function much like an "evidence-detecting divining rod."

152. Pennsylvania v. Mimms, 434 U.S. 106, 108–09 (1977) (per curiam).

153. Tehan v. United States *ex rel.* Shott, 382 U.S. 416 (1966).